3 Privacy and anonymity: Untraceable RFID tags via insubvertible encryption

Giuseppe Ateniese, Jan Camenisch, Breno de Medeiros

November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**

Publisher: ACM Press

Full text available: pdf(238.38 KB) Additional Information: full citation, abstract, references, index terms

We introduce a new cryptographic primitive, called *insubvertible encryption*, that produces ciphertexts which can be randomized without the need of any key material. Unlike plain universal re-encryption schemes, insubvertible encryption prevents against adversarial exploitation of hidden channels, by including certificates proving that the ciphertext can only be decrypted by authorized parties.The scheme can be applied to RFID tags, providing strong protection against tracing. This enables ...

Keywords: RFID privacy, bilinear maps, universal re-encryption

4 Data security for Web-based CAD

Scott Hauck, Stephen Knol

May 1998 **Proceedings of the 35th annual conference on Design automation**

Publisher: ACM Press

Full text available: pdf(198.79 KB) Additional Information: full citation, abstract, references, citings, index terms

Publisher Site

Internet-based computing has significant potential for improving most high-performance computing, including VLSI CAD. In this paper we consider the ramifications of the Internet on electronics design, and develop two models for Web-based CAD. We also investigate the security of these systems, and propose methods for protection against threats both from unrelated users, as well as from the CAD tools and tool developers themselves. These techniques provide methods for hiding unnecessary infor ...

Keywords: Internet, Web-based CAD, data security, encryption

5 Rigorous time/space tradeoffs for inverting functions

Amos Fiat, Moni Naor

January 1991 **Proceedings of the twenty-third annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: pdf(620.73 KB) Additional Information: full citation, references, index terms

6 Verifiable encryption of digital signatures and applications

Giuseppe Ateniese

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

7 A reliable multicast framework for light-weight sessions and application level framing
Sally Floyd, Van Jacobson, Ching-Gung Liu, Steven McCanne, Lixia Zhang
December 1997 **IEEE/ACM Transactions on Networking (TON)**, Volume 5 Issue 6
Publisher: IEEE Press
Full text available: pdf(310.74 KB) Additional Information: full citation, references, citings, index terms, review

Keywords: Internetworking, computer network performance, computer networks

8 Efficient verifiable encryption (and fair exchange) of digital signatures
Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

9 Supporting cryptographic technology: Broadcast encryption with short keys and transmissions
Nuttapong Attrapadung, Kazukuni Kobara
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(269.23 KB) Additional Information: full citation, abstract, references, citings, index terms

Broadcast Encryption allows a broadcaster to broadcast an encrypted message so that only a dynamically changing designated group of users can decrypt it. The stateless setting considers the case where the private key at each user is never updated. A central open problem in this area is to design a stateless scheme where both the size of transmission header which encapsulates the session key and the size of private key at each user are small and *independent* of the number of users (all/priv ...

Keywords: broadcast encryption, constant transmission rate, copyright protection, one-way accumulators, revocation scheme

10 Cryptographic tools: ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption
Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, Anna Lysyanskaya
October 2004 **Proceedings of the 11th ACM conference on Computer and**

communications security

Publisher: ACM Press

Full text available: pdf(220.00 KB) Additional Information: full citation, abstract, references, index terms

A forward-secure encryption scheme protects secret keys from exposure by evolving the keys with time. Forward security has several unique requirements in hierarchical identity-based encryption (HIBE) scheme: (1) users join dynamically; (2) encryption is joining-time-oblivious; (3) users evolve secret keys autonomously.

We present a scalable forward-secure HIBE (fs-HIBE) scheme satisfying the above properties. We also show how our fs-HIBE scheme can be used to construct a forward-secure ...

Keywords: ID-Based encryption, broadcast encryption, forward security

11 Cryptographic tools: Versatile padding schemes for joint signature and encryption

Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, Shabsi Walfish

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(203.91 KB) Additional Information: full citation, abstract, references, index terms

We propose several highly-practical and optimized constructions for joint signature and encryption primitives often referred to as signcryption. All our signcryption schemes, built directly from trapdoor permutations such as RSA, share features such as simplicity, efficiency, generality, near-optimal exact security, flexible and ad-hoc key management, key reuse for sending/receiving data, optimally-low message expansion, "backward" use for plain signature/encryption, long messa ...

Keywords: extractable commitments, feistel transform, joint signature and encryption, signcryption, universal padding schemes

12 Quantum "encryption" (student paper panel)

Mark V. Hurwitz

April 2000 **Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions**

Publisher: ACM Press

Full text available: pdf(107.79 KB) Additional Information: full citation, references, index terms

13 Methods for encrypting and decrypting MPEG video data efficiently

Lei Tang

February 1997 **Proceedings of the fourth ACM international conference on Multimedia**

Publisher: ACM Press

Full text available: pdf(1.45 MB) Additional Information: full citation, references, citings, index terms

Keywords: MPEG codec, compression, multimedia commerce, multimedia encryption, multimedia security

14 A database encryption system with subkeys

George I. Davida, David L. Wells, John B. Kam
June 1981 **ACM Transactions on Database Systems (TODS)**, Volume 6 Issue 2
Publisher: ACM Press

Full text available: pdf(1.16 MB) Additional Information: full citation, abstract, references, citings, index terms

A new cryptosystem that is suitable for database encryption is presented. The system has the important property of having subkeys that allow the encryption and decryption of fields within a record. The system is based on the Chinese Remainder Theorem.

Keywords: data security, databases, decryption, encryption, subkeys

15 Complete characterization of security notions for probabilistic private-key encryption
Jonathan Katz, Moti Yung
May 2000 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available: pdf(973.62 KB) Additional Information: full citation, references, citings, index terms

16 Design of secure cryptography against the threat of power-attacks in DSP-embedded processors
Catherine H. Gebotys
February 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 1
Publisher: ACM Press

Full text available: pdf(214.56 KB) Additional Information: full citation, abstract, references, citings, index terms

Embedded wireless devices require secure high-performance cryptography in addition to low-cost and low-energy dissipation. This paper presents for the first time a design methodology for security on a VLIW complex DSP-embedded processor core. Elliptic curve cryptography is used to demonstrate the design for security methodology. Results are verified with real dynamic power measurements and show that compared to previous research a 79% improvement in performance is achieved. Modification o ...

Keywords: VLIW

17 A public-key cryptosystem with worst-case/average-case equivalence
Miklós Ajtai, Cynthia Dwork
May 1997 **Proceedings of the twenty-ninth annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

18 Encrypt your root filesystem
Mike Petullo
January 2005 **Linux Journal**, Volume 2005 Issue 129
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(24.01 KB) Additional Information: full citation, abstract, index terms

Get high-grade security for all your data even when you can't lock up the hardware.

19 Number-theoretic constructions of efficient pseudo-random functions

Moni Naor, Omer Reingold
March 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 2
Publisher: ACM Press

Full text available: pdf(210.38 KB) Additional Information: full citation, abstract, references, index terms, review

We describe efficient constructions for various cryptographic primitives in private-key as well as public-key cryptography. Our main results are two new constructions of pseudo-random functions. We prove the pseudo-randomness of one construction under the assumption that *factoring* (Blum integers) is hard while the other construction is pseudo-random if the *decisional version of the Diffie--Hellman* assumption holds. Computing the value of our functions at any given point involves tw ...

Keywords: Pseudo-random functions, constant-depth threshold circuits, decision Diffie--Hellman, factoring, learning theory, natural proofs

20 Low power scalable encryption for wireless systems

James Goodman, Anantha P. Chandrakasan
January 1998 **Wireless Networks**, Volume 4 Issue 1
Publisher: Kluwer Academic Publishers

Full text available: pdf(7.39 MB) Additional Information: full citation, abstract, references, index terms

Secure transmission of multimedia information (e.g., voice, video, data, etc.) is critical in many wireless network applications. Wireless transmission imposes constraints not found in typical wired systems such as low power consumption, tolerance to high bit error rates, and scalability. A variety of low power techniques have been developed to reduce the power of several encryption algorithms. One key idea involves exploiting the variation in computation requirements to dynamically vary th ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next